SILVERCORP METALS INC. (the "Company")

CONFIDENTIALITY AND CYBERSECURITY POLICY
(Adopted by the Board on August 6, 2026)

1. POLICY BRIEF & PURPOSE

Our Company's cybersecurity policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store, and manage information, the more vulnerable we become to severe security breaches. Human errors, cyberattacks and system malfunctions could cause great financial damage, operational disruption and may jeopardize our Company's reputation.

For this reason, we have implemented several security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

2. SCOPE

This policy applies to all our employees, employees of subsidiaries and affiliates, contractors and anyone who has permanent or temporary access to our systems and hardware.

3. POLICY ELEMENTS

A. Confidential Data

Confidential data is secret and valuable. To ensure appropriate protection, all employees should take all necessary steps to protect all Company data, including specifically confidential information and do all that is necessary to avoid security breaches.

B. Access Control and Device Security

The Company maintains robust physical and digital shields to protect information.

- **Role-Based Access Control (RBAC):** Data access is granted based on the "principle of least privilege." Permissions are assigned strictly according to job roles and business necessity.
- **Password Integrity:** * Passwords must be at least **eight characters** (including capital and lower-case letters, numbers, and symbols).
- **Authentication:** All systems must be password-protected with two-factor authentication (2FA) enabled where possible. Exchange credentials only when absolutely necessary—prefer the phone over email, and only if you recognize the person.
- **Physical Protection:** Do not leave devices (laptops, tablets, cell phones) exposed or unattended without being locked. Avoid accessing internal systems from public computers (e.g., internet cafés) or lending your devices to others.

C. Network Security

Use the Company-provided VPN when accessing the internet via public networks. Ensure antivirus software and security updates are installed monthly.

D. Reporting Scams, breaches and malware

Our IT service provider needs to know about scams, breaches, and malware so they can better protect our infrastructure. For this reason, we ask our employees to report perceived attacks, suspicious emails, or phishing attempts as soon as possible to our specialists. Our IT service provider will promptly investigate, resolve the problem, and send a Company-wide alert if necessary.

Our IT service provider is responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

E. Data Breach Incident Response

The Company maintains a plan to mitigate the impact of security incidents.

- **Reporting:** Employees must immediately report suspected cybersecurity incidents, unauthorized access, unusual system behavior or suspected data loss to the IT service provider (support@c9s.ca) and the Legal/Compliance Department.
- **Response Workflow:** Upon notification, the Company will activate its response to contain the breach, assess the affected data, and implement recovery.
- **Regulatory Notification:** The Company will comply with all legal requirements for notifying affected parties and regulators (such as the SEC, TSX, or other applicable regulators) within mandated timelines

F. Cross-Border Data Compliance

As a multinational organization operating in jurisdictions such as Canada, China, Kyrgyzstan, and Ecuador, the Company adheres to international data sovereignty laws.

- **Legality Review:** Any cross-border transfer of geological, technical, or sensitive data must undergo a legality review to ensure compliance with local regulations.
- **Partner Responsibilities**: Agreements with foreign partners or contractors must explicitly define the permitted scope of data use, security obligations, and liability for data protection.

G. Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to their manager and IT service provider.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in Company systems.
- Refrain from downloading suspicious, unauthorized, or illegal software on their Company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media and internet usage policy. Our IT service provider should:

- Install firewalls, anti-virus, anti-malware software and access authentication systems.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.

- Follow this policies provisions as other employees do.

Our Company will have all physical and digital shields to protect information.

H. Remote employees

Remote employees must also follow this policy and its instructions. Since they will be accessing our Company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage them to seek advice from our IT service provider.

4. DISCIPLINARY ACTION

We expect all our employees to follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and ask that the employee review policies on security and/or review security training material.
- Intentional, repeated, or large-scale breaches (which causes financial or other damage): We will invoke more severe disciplinary action up to and including termination. We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behavior hasn't resulted in a security breach.

Take security seriously

Everyone should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cybersecurity top of mind.